NATIONAL ARCHIVES AND RECORDS ADMINISTRATION ORGANIZATIONAL ISSUES

HEARING

BEFORE THE

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

JULY 30, 2009

Serial No. 111–70

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.oversight.house.gov

U.S. GOVERNMENT PRINTING OFFICE

58–132 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
MARCY KAPTUR, Ohio
ELEANOR HOLMES NORTON, District of Columbia
PATRICK J. KENNEDY, Rhode Island
DANNY K. DAVIS, Illinois
CHRIS VAN HOLLEN, Maryland
HENRY CUELLAR, Texas
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
PETER WELCH, Vermont
BILL FOSTER, Illinois
JACKIE SPEIER, California
STEVE DRIEHAUS, Ohio

DARRELL E. ISSA, California
DAN BURTON, Indiana
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
BRIAN P. BILBRAY, California
JIM JORDAN, Ohio
JEFF FLAKE, Arizona
JEFF FORTENBERRY, Nebraska
JASON CHAFFETZ, Utah
AARON SCHOCK, Illinois

RON STROMAN, *Staff Director*
MICHAEL MCCARTHY, *Deputy Staff Director*
CARLA HULTBERG, *Chief Clerk*
LARRY BRADY, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

WM. LACY CLAY, Missouri, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
DANNY K. DAVIS, Illinois
STEVE DRIEHAUS, Ohio
DIANE E. WATSON, California

PATRICK T. MCHENRY, North Carolina
LYNN A. WESTMORELAND, Georgia
JOHN L. MICA, Florida
JASON CHAFFETZ, Utah

DARRYL PIGGEE, *Staff Director*

CONTENTS

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION ORGANIZATIONAL ISSUES

THURSDAY, JULY 30, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:40 p.m. in room 2154, Rayburn House Office Building, Hon. Wm. Lacy Clay (chairman of the subcommittee) presiding.

Present: Representatives Clay, McHenry, and Norton.

Staff present: Darryl Piggee, staff director/counsel; Frank Davis, professional staff member; Jean Gosa, clerk; Charisma Williams, staff assistant; Charles Phillips, minority chief counsel for policy; Adam Fromm, minority chief clerk and Member liaison; Howard Denis, minority senior counsel; and Chapin Fay and Jonathan Skladany, minority counsels.

Mr. CLAY. The Information Policy, Census, and National Archives Subcommittee will now come to order.

Good afternoon and welcome to today's hearing entitled, "National Archives and Records Administration Organizational Issues."

Without objection, the Chair and ranking member will have 5 minutes to make opening statements, followed by opening statements not to exceed 3 minutes by any other Member who seeks recognition.

Without objection, Members and witnesses may have 5 legislative days to submit a written statement or extraneous materials for the record.

The purpose of today's hearing is to examine the loss of an external hard drive containing data from the Executive Office of the Clinton administration. We will hear from the Acting Archivist, Adrienne Thomas, and the NARA Inspector General, Paul Brachfeld, and we hope to get real insight into how the security breach occurred and what steps have been taken, and what steps should be taken to tighten security at NARA facilities.

The missing hard drive, which is a backup copy, contained the entire computer files of 113 White House employees. Their entire computer files were downloaded and stored on a hard drive and later transferred to the backup hard drive that is now missing.

Classified documents and personally identifiable information of former Clinton administration staff and visitors to the White House are now exposed.

Before we continue with this hearing, let us be very clear that the subcommittee has no intention of interfering or impeding the investigations currently being conducted by the NARA Inspector General, the Secret Service, or the Federal Bureau of Investigation. We urge everyone's cooperation with these investigations and I thank all of our witnesses for appearing today and look forward to their testimony.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

Statement
Of
Wm. Lacy Clay, Chairman

Information Policy, Census and National Archives
Subcommittee
Oversight and Government Reform Committee

Thursday, July 30, 2009
2154 Rayburn HOB
2:00 p.m.

"National Archives and Records Administration
Organizational Issues"

Good afternoon. Welcome to today's hearing entitled **"National Archives and Records Administration Organizational Issues."**

THE PURPOSE OF TODAY'S HEARING IS TO EXAMINE THE LOSS OF AN EXTERNAL HARD DRIVE CONTAINING DATA FROM THE EXECUTIVE OFFICE OF THE CLINTON ADMINISTRATION. WE WILL HEAR FROM THE ACTING ARCHIVIST, ADRIENNE THOMAS AND THE NARA INSPECTOR GENERAL, PAUL BRACHFELD.

WE HOPE TO GET REAL INSIGHT INTO HOW THIS SECURITY BREACH OCCURRED AND WHAT STEPS HAVE BEEN TAKEN AND WHAT STEPS SHOULD BE TAKEN TO TIGHTEN SECURITY AT NARA FACILITIES.

THE MISSING HARD DRIVE (A BACK-UP COPY), CONTAINED THE ENTIRE COMPUTER FILES OF 113 WHITE HOUSE EMPLOYEES. THEIR ENTIRE COMPUTER FILES WERE DOWNLOADED AND STORED ON A HARD DRIVE AND LATER TRANSFERRED TO THE BACKUP HARD DRIVE THAT IS NOW MISSING. CLASSIFIED DOCUMENTS AND PERSONALLY IDENTIFIABLE INFORMATION OF FORMER CLINTON ADMINISTRATION STAFF AND VISITORS TO THE WHITE HOUSE ARE NOW EXPOSED.

BEFORE WE CONTINUE WITH THIS HEARING, LET US BE VERY CLEAR THAT THE SUBCOMMITTEE HAS NO INTENTION OF INTERFERING OR IMPEDEING THE INVESTIGATIONS CURRENTLY BEING CONDUCTED BY THE NARA INSPECTOR GENERAL, THE SECRET SERVICE OR THE FEDRAL BUREAU OF INVESTIGATION (FBI). WE URGE EVERYONE'S COOPERATION WITH THESE INVESTIGATIONS.

I THANK ALL OF OUR WITNESSES FOR APPEARING TODAY AND LOOK FORWARD TO THEIR TESTIMONIES.

Mr. CLAY. Now, we are on a tight schedule today, so what I am going to do is, normally we would yield to the ranking member, who is not here yet. When he gets here, he will be allowed an opening statement, but I will swear the witnesses in. I will introduce you and swear you in, and hopefully by the end a minority Member will be here.

Let me first introduce the panel. We will hear first from Ms. Adrienne Thomas, Acting Archivist of the U.S. National Archives and Records Administration. Ms. Thomas is currently the Acting Archivist of the United States. Prior to her appointment as Acting Archivist in December 2008, Ms. Thomas served as the Deputy Archivist of the United States.

Ms. Thomas has been with the National Archives for 38 years, beginning as an Archivist Trainee in the Office of Presidential Libraries, and subsequently holding a number of policy and administrative roles.

Ms. Thomas will be accompanied by Mr. Gary M. Stern, General Counsel for the National Archives and Records Administration.

Welcome to both of you.

Our next witness will be Mr. Paul Brachfeld, Inspector General, National Archives and Records Administration. Mr. Brachfeld serves as the IG of NARA and as the IG for NARA, he oversees the conduct and execution of all audits, investigations and inspection for the agency, in compliance with provisions of the Inspector General Act of 1978 as amended.

Mr. Brachfeld's entire career has been devoted to investigative activities since graduating from the University of Maryland College Park in 1979. Go Terps. And today, he brings 10 years of experience as the NARA Inspector General and 30 years of exceptional service to the U.S. Government. Currently at NARA, Mr. Brachfeld's tenure has included the recovery of hundreds of stolen archival holdings and related successful prosecutions of identified subjects. And we look forward to his testimony.

I want to welcome all of you to our hearing today, and it is the policy of the Oversight and Government Reform Committee to swear in all witnesses before they testify.

Would all of you please stand and raise your right hands?

[Witnesses sworn.]

Mr. CLAY. You may be seated. Thank you.

Let the record reflect that the witnesses answered in the affirmative, and each of you will have 5 minutes to make opening statements. Your complete written testimony will be included in the hearing record. The yellow light will indicate that it is time to sum up. The red light will indicate that your time has expired.

Ms. Thomas, you may begin your opening statement.

STATEMENTS OF ADRIENNE C. THOMAS, ACTING ARCHIVIST OF THE UNITED STATES, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, ACCOMPANIED BY GARY M. STERN, GENERAL COUNSEL, THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, AND SHARON THIBODEAU, DEPUTY ASSISTANT ARCHIVIST FOR RECORDS SERVICES; AND PAUL BRACHFELD, INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

STATEMENT OF ADRIENNE C. THOMAS

Ms. THOMAS. Thank you, Chairman Clay and members of the subcommittee. I appreciate this opportunity to discuss a recent security incident that is a serious breach of the trust placed in the National Archives to protect our Nation's records.

NARA learned in late March that an external computer hard drive containing copies of Clinton Administrative Executive Office of the President records was missing from the electronic records processing room. As the Acting Archivist, and as someone who has devoted my entire 39-year career to the National Archives, I am deeply angered that a NARA employee or contractor may have intentionally removed this item.

With me today are NARA's General Counsel and Senior Agency Official for Privacy, Gary Stern, and Sharon Thibodeau, Deputy Assistant Archivist for Records Services.

The loss of the hard drive occurred while NARA was conducting preservation processing of electronic media received from the Executive Office of the President [EOP], at the end of the Clinton administration. Tapes containing snapshots of the contents of the working drives of EOP employees were copied by a contractor to new media to prevent deterioration.

On September 18, 2008, two My Book hard drives created by the contractor were delivered to NARA. The hard drives were labeled master No. 2 and backup No. 2. The two hard drives were taken to suite 5300 at the National Archives in College Park and placed on a shelf in the unclassified electronic records processing room within the suite. At the time, approximately 85 NARA employees and contractors had badges that opened the three doors to the office area of the suite. Individuals with badge access to suite 5300 also had access to the electronic records processing room for unclassified records.

On October 30th, the work of verifying the records on the hard drive was assigned to an information technology specialist. Work was performed only on the master No. 2 hard drive, not the backup No. 2, which would later be missing.

On February 5, 2009, the IT specialist placed the master No. 2 hard drive into its original manufacturer's box and noted that the backup No. 2 hard drive was in a similar adjacent box. The two boxes remained on a shelf in the processing room and no additional work was done on the hard drive until March 24, 2009, when the IT specialist discovered that the box that had contained backup No. 2 hard drive was empty. The master No. 2 hard drive was still in its box.

An immediate division-wide search was initiated. On April 2, 2009, the Inspector General, General Counsel and I were informed

of the loss. While the Office of the Inspector General continues its investigation, there are currently no facts to determine whether the drive was stolen or misplaced and no suspect has been identified. NARA has offered a reward of up to $50,000 for information that leads to the recovery of the missing hard drive.

NARA staff reviewed the master No. 2 hard drive and discovered that it contained numerous files containing personal names and Social Security numbers. In addition, NARA also found a small number of files that contained markings indicating they may contain classified information. While information from the EOP provided at the time of transfer indicated that the hard drives did not contain classified data, we believe EOP employees must have accidentally or improperly stored some classified information on their unclassified computers.

We are compiling a list of those individuals who may have had their personal information compromised and a credit monitoring contractor is notifying these individuals as they are identified. To date, approximately 15,750 notification letters have been mailed. NARA is offering each individual 1 year of free credit monitoring services and fraud protection. To date, 796 individuals have signed up for the credit monitoring services. Because of the extremely large volume of data on the drive, over 8.7 million individual files, we do not yet know the total number of individuals whose privacy has been affected.

NARA has taken steps to improve internal security in our Electronic Records Division. First, we have added separate bad access controls to the doors opening the processing rooms in suite 5300. There are now only entrances to the processing room and only individuals with badges programmed to open these doors may enter the processing room. All others must sign the log and be accompanied by an authorized person while in the room.

Second, we conducted an audit of all electronic media containing personally identifiable information and moved it to a separate locked block of shelving within a locked stack area accessible only to authorized employees.

Finally, all NARA staff are required to complete training on how to handle sensitive information, including the new security procedures.

The Office of Records Services is also conducting unannounced inspections of all records branches and divisions on a periodic basis, and supervisors are required to do periodic walk-through inspections during the day.

When the investigation of this incident by NARA's Office of Inspector General and Secret Service is completed, I can assure you that we will act on the results with swift and appropriate disciplinary actions if it is determined that any NARA employees were responsible for removing the hard drive or failed to adhere to proper records handling procedures.

The National Archives is a public trust and the 3,000 women and men who work at NARA's 44 facilities across the country take their job and that trust very seriously. Every day, our staff performs work that is vital to our democracy by preserving and safeguarding the more than 9 billion records that make up the National Archives of the United States.

At the same time, we must balance safeguarding the records with providing the people of this country access to those records. As with any endeavor that relies on the work of human beings, our work, despite our best efforts and intentions, is subject to error. However, the loss of even one record or breach, even one individual's personal information is unacceptable. And I assure you that NARA will continue to improve our security procedures and ensure that all staff is inculcated with the importance of following these procedures.

Given the seriousness with which we take this loss, I am thankful for the opportunity to testify and I will try to answer any questions that you may have.

[The prepared statement of Ms. Thomas follows:]

Testimony
Of
Adrienne Thomas
Acting Archivist of the United States

Information Policy, Census, and the National Archives
Subcommittee
Oversight and Government Reform Committee

Thursday, July 30, 2009
2154 Rayburn HOB
2:00 p.m.

"National Archives and Records Administration Organizational Issues"

Introduction

Chairman Clay, Ranking Member McHenry and members of the Subcommittee, I am Adrienne Thomas, Acting Archivist of the United States and I appreciate being given this opportunity to appear before you to discuss a recent security incident which is a serious breach of the trust placed in the National Archives to protect our nation's records. As you know Mr. Chairman, we have kept your staff apprised of this issue, and we were very pleased that a group of staff were able to come to our College Park facility two weeks ago to get a first-hand briefing and tour of the location of this incident.

The National Archives and Records Administration (NARA) learned in late March 2009 that an external computer hard drive containing copies of Clinton Administration Executive Office of the President (EOP) Presidential and Federal records was missing from a NARA electronic records processing room. The Office of the Inspector General continues to investigate who was responsible for the disappearance of the hard drive. As the Acting Archivist, but also as someone who has devoted my entire 39 year career to the National Archives, I am deeply angered that a NARA employee or contractor may have intentionally removed this item, and I am disappointed that our procedures as implemented were not sufficient to forestall this incident.

In the testimony below, I will describe the circumstances and events surrounding the loss of a hard drive for which we were responsible and I will describe the steps we have taken to ensure that such a loss does not occur again. Since this hard drive contained personally identifiable information (PII), with me today is NARA's General Counsel and Senior Agency Official for Privacy, Gary M. Stern, who can respond to any questions

you have about our efforts to inform individuals about the potential compromise of their personal information. In the event that you have specific questions which I cannot answer in regard to the operations and security of the NARA work area where this incident occurred, seated behind me is Sharon Thibodeau, Deputy Assistant Archivist for Records Services, who is prepared to provide these details.

The role of the National Archives and Records Administration is to serve as the nation's record keeper and to make those records as broadly accessible as possible, while balancing such access with the need to protect national security, personal privacy, and other sensitive information. We accession approximately 3 percent of all federal records—those deemed most important, with the greatest long-term value – and all Presidential records.

These records remain important long after they are no longer needed for the original purpose they were created. Americans come to our facilities all around the country to examine them—to trace their family roots, to verify Federal military or civilian service, to prepare for legal proceedings, to hold the agencies and their officials accountable for carrying out their role in serving the American people, and to enable historians to write another chapter of the history of our country.

Over the past 75 years, most of those records have come to us on paper. Today, these records total almost 9 billion pieces of paper archived in our facilities nationwide. They include acts of Congress, documents of individual departments and agencies, papers of Presidents, material from cases decided by the federal courts, and the personnel records of 56 million veterans of our armed forces. Besides text documents, we also have maps of land and sea, 14 million photographs of all kinds, and large audio and visual holdings.

Although our first accession of electronic records dates to 1969, the volume and complexity of electronic records has increased dramatically. Over the past decade, we have been getting new kinds of records from all across the Federal government: electronic text documents, e-mails, snapshots of web pages, digital images, spreadsheets, presentations, audio and video data files, databases, satellite imagery, geographic information systems, and more. The future will bring records created on Personal Digital Assistants and Internet features such as Blogs and Facebook pages of Federal agencies.

These new kinds of records present new challenges for us. They are coming to us on an increasing variety of hardware and storage devices—often physically smaller and more complex but able to hold more information. For example, in its first year of operation 75 years ago, the National Archives took in the equivalent of 8 million documents—58,794 cubic feet of records. Today, those 8 million documents would fit on a single portable electronic storage device. The concentration of so much data on a piece of equipment the size of a novel presents significant challenges that the original archivists in 1934 could not imagine. We must be even more vigilant in ensuring that our security protection measures are in place and being implemented by today's Archives staff.

Meeting these challenges is of paramount concern to the National Archives, but they are challenges we must take on with vigor because of the ever expanding opportunities to provide the American people – regardless of where they live – with access to the records that document our democracy, our rights and the story of our nation. But as with any endeavor that relies on the work of human beings, we will, despite our best efforts and best intentions, occasionally make mistakes along the way. While only a small portion of our holdings are truly sensitive, any error in our management of these sensitive records is unacceptable and we will learn from our mistakes to become better at what we do by encouraging an environment of continuous improvement.

Now I will describe a loss of data from which we must learn much, so that it does not happen again.

Background

The loss of the hard drive occurred while NARA was conducting preservation processing of electronic media that we had received from the Executive Office of the President (EOP) at the end of the Clinton Administration. In accordance with the Presidential Records Act, the EOP transferred the official electronic records of the Clinton Administration in 2001. While most records transferred from the EOP are received and processed by the staffs of the Presidential Libraries, records in electronic form have, since the Reagan Administration through the Clinton Administration, been transferred for preservation to NARA's Electronic and Special Media Records Services Division, which is located organizationally within the Office of Records Services in our facility in College Park, MD.

In addition to official electronic records from the Clinton Administration, NARA also received from the EOP over 60,000 electronic storage items consisting of backup tapes and work media, additional copies of files restored from the backup tapes, snapshots of employee working drives on various 4mm and 8mm tape formats, and actual hard drives from the Clinton EOP. The material from the EOP included units that fell under the requirements of either the Federal Records Act (FRA) or the Presidential Records Act (PRA) and included both classified and unclassified materials.

As part of NARA's responsibility to ensure that electronic materials are preserved until such time as their final disposition is determined, NARA identified a subset of approximately 2,500 tapes and four hard drives from the Clinton EOP, known as "reallocation tapes," for re-copying. Such re-copying is consistent with our regulatory requirement that electronic tape media at least 10 years old should be copied to new media to prevent deterioration. Essentially the reallocation tapes contained "snapshots" of the contents of the working drives of departing EOP employees, which were originally created and preserved to fulfill the requirements of pending litigation.

These tapes consisted of a wide variety of 4mm, 8mm, and QIC (quarter inch cartridge) tape formats, and most of the tapes could not be read by NARA tape drives. Therefore,

NARA sought vendors that could read the tapes and copy them onto formats compatible with NARA's electronic records preservation systems starting in Fiscal Year 2005. Over the course of four years NARA had three different companies under four separate contracts conduct preservation copying on a portion of this media. In July 2005, NARA contracted with Arkival Technology Corp. Arkival Corp copied 437 tapes onto digital linear tape (DLT) media. In April 2006, Arkival Corp copied another seven tapes and four hard drives onto DLT media. Later in Fiscal Year 2006, Muller Media Conversions copied 277 tapes onto DLT media. In Fiscal Year 2007, Arkival copied 300 tapes onto two one-terabyte My Book hard drives, which, as the name implies, are about the physical size of a paperback book. Arkival subsequently made an additional set of back up copies of the hard drives for a total of four hard drives.

In Fiscal Year 2008, NARA contracted with RICOMM Systems, Inc, to copy 1,428 tapes. RICOMM to date has copied 881 tapes onto eight two-terabyte My Book hard drives. As with the Arkival contract, RICOMM also made a backup copy of each of the 2 terabyte hard drives for a total of sixteen My Book hard drives. Two of these RICOMM-created My Book hard drives were delivered to NARA on September 18, 2008. They were labeled "Master #2" and "Backup #2." Records show that each of these drives contained copies of data from 113 of the Clinton Administration "reallocation tapes" designated for preservation copying. The missing hard drive about which we are testifying today is the hard drive that was labeled "Backup #2."

Incident

On the day of their delivery to NARA, the RICOMM-created hard drives Master #2 and Backup #2 were taken to a work station within suite 5300 of the NARA facility in College Park, MD. An Information Technology Specialist, GS-13, Team Leader verified the paperwork received from the contractor and confirmed that we received the correct hard drives.

Suite 5300, which Oversight Committee staff visited two weeks ago, contains offices, work cubicles arranged in an open configuration, and separate, enclosed unclassified, classified, and Census electronic records processing rooms. There are three doors opening into the suite, two front doors and a back door, each of which is controlled by an electronic card key system. All of the controlled doors to suite 5300 are within NARA's general perimeter security system. At the time of receipt of Master #2 and Backup #2, approximately 85 individuals (NARA employees and contractors) had badges that activated the card key system controlling the doors to suite 5300. Although separately enclosed, the unclassified electronic records processing room had no additional security. Individuals with badge access to suite 5300 also had access to the electronic records processing room. In fact, one of the three doors into the suite, the back door, opens directly into the electronic records processing area

At the time of receipt of Master #2 and Backup #2, the back door to suite 5300, the one opening directly into the unclassified electronic records processing room, was sometimes held open to allow for better ventilation in that room. This occured because the large

number of electronic devices operating in the room could elevate its temperature to problematic levels. Staff members were instructed never to open the door for ventilation purposes unless an authorized staff member was always present in the area. I will describe the security enhancements that have been made since the loss of the hard drive later in this testimony.

On September 23, after NARA staff verified receipt of the drives, they were placed in the unclassified electronic records processing room in Suite 5300 where staff would then verify that the contractor had completed the work. The IT Specialist Team Leader created a map of the Master #2 hard drive that describes the directory structure of the disk. The hard drives were placed on a shelf in the unclassified electronic records processing room of Suite 5300, and on October 30, 2008, the work of processing the records on the hard drive was assigned to a GS-11 Information Technology Specialist. The IT Specialist was instructed to compare the actual file structure of the disk to the map that the IT Specialist Team Leader had produced, print out the first five pages of each file on the disk, and compile the printouts in folders without examining the contents of the printouts. Work was performed only on the Master #2, not the Backup #2 (which would later be missing from the processing room).

Normally electronic media in the custody of NARA are housed in storage areas called stacks which have limited access. Standard operating procedures call for staff members to check out media from the storage area, process the records in the appropriate electronic records processing room and return the records to the storage area at the end of the day. In addition, when the contents of the media are determined to have sensitivities, such as personally identifiable information, NARA stores the records in areas with an additional level of security. In the case of the missing hard drive, the hard drives were not returned to the storage area at the end of the day. The staff member performing the preservation copying of the hard drive had no knowledge of the contents of the media and thus did not know that it contained personally identifiable information. That was only determined later when the hard drive disappeared and the content of Master #2 was examined. Nevertheless, the hard drive had characteristics that made it vulnerable to theft, such as a high storage capacity (two terabytes) and portability. When not being processed, both hard drives should have been placed in a storage area with an additional level of security.

Work on Master #2 stopped on January 30, 2009. Because of the voluminous amount of paper generated as a result of printing out the first five pages of each file, the IT Specialist Team Leader halted the project in order to investigate an automated way to validate the hard drive directory structure. On February 5, 2009, the IT Specialist working on the project placed the Master #2 into its box located near the work station. The IT Specialist noted that Backup #2 was also securely housed in a box adjacent to Master #2.[1] The two boxes which should have contained the two hard drives remained on a shelf located above the electronic records processing work station in the unclassified electronic records processing room until March 24, 2009. During this time period, no one reported opening the boxes and viewing their contents.

[1] The Office of the Inspector General has informed us that when they interviewed the staff member, the staff member could not be 100% certain that Backup #2 was in the box on February 5.

We should also note at this time that NARA backs up its electronic records processing system data onto high density, portable hard drives. One brand NARA uses is the one-terabyte version of the Western Digital My Book line of hard drives, which is similar in appearance to the two-terabyte version that is missing. Because the hard drives had no distinctive marking as containing record materials, staff members not familiar with the EOP preservation project might erroneously have thought that the hard drives containing the EOP material were media used for system backups, and therefore assumed that they were properly stored in the processing room. We do not offer this as an excuse for the improper handling of the hard drive, but simply as an explanation for why it may have taken a long period of time before staff discovered the hard drive missing. It also demonstrates a potential challenge in our inventory procedures that we must consider as we move forward from this incident.

With the new software procured and tested, on March 24, 2009, the IT Specialist originally assigned to work on Master #2 and Backup #2 returned to work on these media and discovered that the box that had contained the hard drive labeled as Backup #2 was empty. The adjacent box was found to contain the hard drive labeled Master #2. The IT Specialist informed the IT Specialist Team Leader and the IT Specialist Team Leader informed the Supervisor that a loss had occurred. The IT Specialist Team Leader and Supervisor immediately began a search for the missing hard drive, Backup #2. They checked all of the workstations and rooms within Suite 5300 and the stack area normally used to house electronic media. They also checked other work spaces occupied by the division. They did not find hard drive Backup #2.

On March 27, 2009, they informed the Director of the Electronic and Special Media Records Services Division (NWME) of the apparent loss. The Director commenced a division-wide search which did not produce results. Staff thoroughly searched the processing rooms and the stack areas where original and back-up media are stored. Staff working in the unclassified processing room was also questioned about their knowledge of the hard drive. On March 31, 2009, the Supervisor submitted a report of the loss to the NWME Division Director. On April 1, 2009, the Division Director informed NARA security and other staff members within the Office of Records Services, Washington, DC including the Assistant Archivist who manages the Office. On April 2, 2009, I, NARA's Inspector General, and NARA's General Counsel were informed of the loss.

Response and Investigation

While NARA employees searched for hard drive Backup #2, staff also began to review hard drive Master #2 in order to determine whether it (and its missing counterpart, Backup #2) contained any sensitive information, such as personally identifiable information. After performing a number of key word searches of hard drive Master #2, NARA discovered that there were numerous files containing personal names and social security numbers. The hard drive contained the contents of the working drives of EOP staff members and, as such, represented a snapshot of the administrative work conducted by the staff of the EOP. The administrative work included managing personnel actions,

payroll, White House visits, and other administrative matters. In addition, NARA also found a small number of files that contain markings indicating that they may contain information that was classified at the time of creation. While transfer information from the EOP indicated that the hard drives did not contain classified data, we believe the presence of what may be classified information occurred when EOP employees accidentally or improperly stored classified information on their unclassified computers. The OIG has the lead responsibility for facilitating the declassification review process to determine if any of these files contain information that should remain classified.

In accordance with OMB requirements, NARA immediately reported the missing hard drive Backup #2 to the U.S. Computer Emergency Readiness Team of the Department of Homeland Security as a potential breach of personally identifiable information. NARA also notified staff of our House and Senate Oversight Committees, the White House Counsel's Office, and the representative of former President Clinton. In addition, NARA convened our Breach Response Team in order to determine how to respond to the breach of the PII.

The Office of Inspector General immediately commenced an investigation to determine who was responsible for removing the hard drive, which remains ongoing. We have been advised by the OIG that there are currently no facts to determine whether the drive has been stolen or was misplaced, and no suspect has been identified.

NARA also immediately moved all previously copied hard drives with EOP content and original EOP tapes to classified storage. Further, NARA has offered a reward of up to $50,000 for information that leads to the recovery of hard drive Backup #2.

NARA has made a copy of Master #2 and is currently reviewing the data on it to compile a list of those individuals who may have had their personal information compromised. Through the services of a credit monitoring contractor, NARA has begun to send out letters to these individuals as they are identified. To date, approximately 15,750 letters have been mailed. The letters also have an enclosure that provides individuals with information regarding the breach and ways for those individuals to protect themselves. In addition, NARA is offering each individual one year of free credit monitoring services and fraud protection. Further, NARA has set up a Breach Response Call Center and a Breach Response email box, which are fielding inquiries from individuals requesting additional information. We have also posted information about this matter on our website, at www.archives.gov. Because of the extremely large volume of data on the drive – over 8.7 million individual files – we do not yet know the total number of individuals whose privacy has been affected. Breach notification letters will be sent to individuals as they are identified.

Changes made as a result of the loss

NARA has taken several steps to improve internal controls in the following areas: physical security of the electronic records processing workspace and treatment of electronic devices containing personally identifiable information.

First, NARA has completely separated access to the unclassified electronic records processing room from access to suite 5300. The entrance to suite 5300 that had opened directly into the processing room is no longer operational as a suite entrance. This door is being equipped with emergency exit hardware which will sound an alarm if a person opens it for any reason. (The ventilation concerns that had led to instances of opening this door have been addressed by installation of improved air handlers in the room.) Individuals who need access to the unclassified electronic records processing room are limited to entering the room from doors inside suite 5300. These processing room doors now have separate card key access systems and only individuals with badges programmed to open these doors may enter the room. Individuals without badge access to the processing room must be authorized by a NARA manager, sign a log prior to entry, and be escorted while in the room by an individual with badge access.

Second, we conducted an audit of all physical media, for example, magnetic tapes, CDs, hard drives, and similar portable devices containing PII and other sensitive information (including Presidential EOP media). Those devices identified as containing this type of information were moved to a separately secured storage area where only those employees who handle such materials have access. Access to this protected space, which is located within the secure stack storage area housing unclassified electronic records (which your staff also visited two weeks ago), is granted only to employees authorized access to sensitive records, including PII. The employees identify the material being withdrawn and log the movement of the material in and out of the storage area on a separate media log. A supervisor must ensure compliance by reviewing the sign-in logs and inspecting the processing and storage areas on a daily basis.

Finally, all NARA staff is required to take two courses on how to handle sensitive information: Personally Identifiable Information training and Information Assurance Awareness training. In addition, the staff of the Electronic and Special Media Records Services Division was trained on the new procedures described above and sensitized to returning records to proper storage areas when not in use.

Conclusion

As the Subcommittee knows, the investigation of this incident is ongoing under the direction of NARA's Office of Inspector General. Additionally, the United States Secret Service has assisted in providing forensic IT support to NARA's Office of the Inspector General. While I cannot comment on the investigation, I can assure you that the results of that investigation will be taken very seriously by me and swift and appropriate disciplinary actions will be taken if it is determined that any NARA employees were responsible for removing the hard drive or failed to adhere to proper records handling procedures.

NARA is a public trust, and the 3,000 women and men who work at NARA facilities across the country take their jobs, and that public trust, very seriously. In this year, in which NARA celebrates 75 years of service to the nation, I wish I was up here today to

testify about all of the vital work we do every day to preserve and protect, while providing public access to, over 9 billion – and growing – pages of records. Given the seriousness with which we take this loss, however, I am thankful to you for giving me the opportunity to testify and I would be happy to answer any questions.

Mr. CLAY. Thank you so much, Ms. Thomas.
Mr. Brachfeld, you are up next.

STATEMENT OF PAUL BRACHFELD

Mr. BRACHFELD. Mr. Chairman and members of the subcommittee, I thank you for offering me the opportunity to testify today. I have been called before the subcommittee to provide testimony on the circumstances surrounding an external computer hard drive missing from the National Archives and Records Administration which contained a vast amount of material from the Clinton administration, including Presidential Record Act [PRA], material.

The Presidential Record Act of 1978 governs the official records of the President and Vice President created or received after January 20, 1981. The PRA changed the legal ownership of the official records of the President from private to public and established a new statutory structure under which Presidents must manage their records.

I trust that in reaction to the loss of a hard drive, new policies, procedures and processes will be defined and implemented at NARA, and certainly my office will evaluate these actions, provide guidance and appropriate independent and skilled oversight.

However, our focus now is on the criminal investigation of the disappearance of the hard drive capable of holding two terabytes of our government's information, and which my forensic investigator informs me was essentially filled with data.

At the outset, I must say I am not able to talk about all aspects of the investigation at this time. This is an ongoing criminal investigation which may have elements affecting national security. Therefore, I know that the Chair and members of this distinguished committee would not wish me to provide any information that could potentially damage the investigation's integrity or potential success.

Currently, we are working with the assistance of the U.S. Secret Service and the Federal Bureau of Investigation to more precisely identify the content of the hard drive. However, an initial cursory review identified that thousands of examples of personally identifiable information [P.I.] data, reside on the hard drive. We reported this to NARA management officials and they have hired a contractor to further analyze this P.I. aspect and provide breach notification per OMB requirements.

I should also note that at my request, the Special Agent in charge of the Secret Service Washington Field Office generously made their 24/7 hotline operation available to us in order to support the investigation and potential recovery of the missing drive.

In response to our suggestion, NARA has established a reward of up to $50,000 for information leading to the successful recovery of the missing hard drive. No productive leads have resulted to date from this action.

The subcommittee has asked about the security in place at NARA at the time the hard drive went missing and after the hard drive went missing. The direct answer is that the controls in place were inadequate and what controls were in there were readily bypassed and obviously compromised on an ongoing and dynamic

basis. Quite simply, this was an accident waiting to happen and now it has.

As a direct result of these failures in controls, my office's capacity to investigate this incident has been severely compromised. The loss went unnoticed potentially for months. Conservatively speaking, at least 150 people had access to the area, and even rudimentary access controls such as badge or sign-in logs were not maintained or could be readily bypassed.

While the drive was kept in an area ostensibly secured by a proximity card-reading lock, in practice this system failed. People could simply piggyback by going through the door when other persons opened it, and even worse, doors which should have been secured were propped open for ventilation purposes.

It was also reported to my investigators that the processing area in which the hard drive went missing was used as a conduit or shortcut to the rest rooms. Therefore, it can be argued that the security for this area was no greater than the general security for the building as a whole.

The loss of this hard drive holding PRA materials is not the only concern I have in this investigation. Many in the pool of potential subjects of this criminal investigation have access to the processing area where this drive disappeared, as well as more traditional storage or stack areas. Therefore, I cannot say with any confidence that data stored in these areas was not compromised. This includes the records of the 9/11 Commission, the Warren Commission, as well as large quantities of other national security holdings.

In a benign case where proper controls were in place and a subject hard drive was lost or ruinously disposed of, one might take comfort that other data was not compromised. The facts dictate that I am afforded no such comfort. If the drive was deliberately removed, the person or persons could have just as readily removed other holdings or copied information onto other mediums.

I am also deeply concerned about how NARA generally treated the category of Presidential data like that which was on the missing hard drive. Specifically, when the data was copied from original Executive Office of the President [EOP] computer tapes to modern hard drives, the copying was done by contractors offsite without any security requirements. NARA had a fixed price delivery order for the duplication of 1,428 such EOP computer tapes to external hard drives to include the missing hard drive.

A small business was provided complete custody and control over the housing content of the EOP material. Amazingly, this contractor was one in a series of like contracts in which NARA was silent in addressing any security requirements for the tapes or the information which they held. In fact, the contractor made absolutely no mention of the sensitivity of these records, nor included a nondisclosure agreement.

When handling and processing groups of PRA material, I would think it essential to institute appropriate measures for security over transport and processing of these records offsite by contractors. However, no such measures were identified. In this specific case, the tapes were sent offsite to a small storefront operation in New Jersey. The existing security at this location was rudimentary

and clearly inadequate to protect and limit inappropriate access to PRA material.

In a June 18, 2009 letter, Senator Charles E. Grassley asked the Acting Archivist of the United States: "Do you recognize NARA is a national security agency?" She stated, "No. NARA is not a national security agency by any shared means of that term within the executive branch for which we are aware. NARA does not make nor does it implement national security policy. NARA's only relationship to national security is our responsibility for ensuring that those security classified records that come into our custody from other agencies are stored, protected and handled following the rules for which all agencies that handle classified records must adhere."

I would submit that NARA has in this and other recent cases breached that relationship. While by some technical standards, NARA may not meet the traditional definition of a formal national security agency, the information and records we hold are vital to our Nation's security.

What I will say specific to the loss of this hard drive is that the American people deserve better security and accountability than NARA has provided them. I can assure you that through our audits and investigations, management consultations and briefings, we will work to help NARA strengthen its internal control and security mechanism.

While some corrective measures have, and I trust more will be taken, it is analogous to closing the barn door after the horse has left. The event has passed and damage done, the extent to which I cannot quantify for you today.

I thank you for the opportunity to testify and am available to take questions.

[The prepared statement of Mr. Brachfeld follows:]

Statement

Of

Mr. Paul Brachfeld

Inspector General

National Archives and Records Administration

Information Policy, Census, and National Archives Subcommittee

Oversight and Government Reform Committee

Thursday, July 30, 2009

2154 Rayburn HOB

2:00 p.m.

"National Archives and Records Administration Organizational Issues"

Mr. Chairman and Members of the Subcommittee, I thank you for offering me the opportunity to testify today.

I have been called before the Subcommittee to provide testimony on the circumstances surrounding an external computer hard-drive missing from the National Archives and Records Administration (NARA) which contained a vast amount of material from the Clinton Administration including Presidential Records Act or PRA material. The Presidential Records Act (PRA) of 1978, 44 U.S.C. ß2201-2207, governs the official records of Presidents and Vice Presidents created or received after January 20, 1981. The PRA changed the legal ownership of the official records of the President from private to public, and established a new statutory structure under which Presidents must manage their records. I trust that in reaction to the loss of the hard-drive new policies, procedures, and processes will be defined and implemented at NARA, and certainly my office will evaluate these actions to provide guidance and appropriate independent and skilled oversight. However our focus now is on the criminal investigation of the disappearance of a hard-drive capable of holding two terabytes of our government's information, and which my forensic investigator informs me was essentially filled with data. At the outset, I must say I am not able to talk about all aspects of the investigation at this time. This is an ongoing criminal investigation which may have elements affecting national security; therefore, I know that the Chair and distinguished members of

the subcommittee would not wish me to provide any information that could potentially damage the investigation's integrity or potential success.

Currently we are working with the assistance of the United States Secret Service and the Federal Bureau of Investigation to more precisely identify the contents of the hard-drive. However, an initial cursory review identified that thousands of examples of personally identifiable information or PII data resided on the hard-drive. We reported this to NARA management officials and they have hired a contractor to further analyze this PII aspect and provide breach notifications per OMB requirements. I should also note that at my request the Special Agent In Charge of the Secret Service Washington Field Office generously made their 24/7 hotline operation available to us in order to support the investigation and potential recovery of the missing drive. In response to our suggestion NARA established a reward of up to $50,000 for information leading to the successful recovery of the missing hard-drive. No productive leads have resulted to date from this action.

The subcommittee asked about the security in place at NARA at the time the hard-drive went missing, and after the hard-drive went missing. The direct answer is that the controls in place were inadequate, and what controls were there were readily bypassed and obviously compromised on an ongoing and dynamic basis. Quite simply, this was an accident waiting to happen, and now it has.

As a direct result of these failures in controls, my office's capacity to investigate this accident has been severely compromised. The loss went unnoticed potentially for months; conservatively speaking at least 100 people had access to the area; and even rudimentary access controls such as badge or sign-in logs were not maintained or could be readily bypassed. While the drive was kept in an area ostensibly secured by a proximity card reading lock, in practice this system failed. People could simply piggy-back by going through the door when another person opened it; and even worse, doors which should have been secured were propped open for ventilation purposes. It was also reported to my investigators that the processing area in which the hard-drive went missing was used as a conduit or short-cut to the restrooms. Therefore it can be argued that the security for this area was no greater then the general security for the building as a whole.

The loss of this hard-drive holding PRA material is not the only concern I have in this investigation. Many in the pool of potential subjects of this criminal investigation have access to the processing area, where this disk-drive disappeared, as well as to more traditional storage or stack areas. Therefore, I cannot say with any confidence that data stored in these areas was not compromised. This includes the records of the 9/11 Commission, the Warren Commission as well as large quantities of other national security holdings. In a benign case where proper controls were in place or the subject hard-drive was lost or erroneously disposed of, one might take comfort that other data was not compromised. The facts dictate that I am afforded no such comfort. If the drive

was deliberately removed, the person or persons could have just as readily removed other holdings or copied information onto other mediums.

I am also deeply concerned about how NARA generally treated the category of presidential data like that which was on the missing hard-drive. Specifically, when the data was copied from original Executive Office of the President or EOP computer tapes to modern hard-drives, this copying was done by contractors – off-site and without any security requirements. NARA had a fixed-price delivery order for the duplication of 1,428 such EOP computer tapes to external hard-drives to include the missing hard-drive. A small business was provided complete custody and control over the housing and content of this EOP material. Amazingly, this contract was one in a series of like contracts in which NARA was silent in addressing any security requirements for the tapes or the information which they held. In fact, the contract made absolutely no mention of the sensitivity of the contents of these records.

When handling and processing groups of PRA material, I would think it essential to institute appropriate measures of security over transport and processing of these records off-site by a contractor. However, no such measures were identified. In this specific case the tapes were sent off-site to a small store-front operation in New Jersey. The existing security at this location was rudimentary and clearly inadequate to protect and limit inappropriate access to PRA material.

In a June 18, 2009 letter, Senator Charles E. Grassley asked the Acting Archivist of the United States, "Do you recognize NARA as a National Security Agency?" She stated "No. NARA is not a national security agency by any shared meaning of that term within the Executive Branch for which we are aware. NARA does not make nor does it implement national security policy. NARA's only relationship to national security is our responsibility for ensuring that those security classified records that come into our custody from other agencies are stored, protected, and handled following the rules to which all agencies that handle classified records must adhere."

I would submit that NARA has in this and other recent cases breached that relationship. While by some technical standards NARA may not meet the traditional definition of a formal National Security Agency, the information and records we hold are vital to our nation's security. What I will say specific to the loss of this hard-drive is that the American people deserve better security and accountability then NARA has provided them. I can assure you that through our audits and investigations, management consultations and briefings, we will work to help NARA strengthen its internal control and security mechanisms.

While some corrective measures have, and I trust more will be taken – it is analogous to closing the barn door after the horse has left. The event has passed and the damage done, the extent of which I cannot quantify for you today.

I thank you for the opportunity to testify and am available to take your questions.

Mr. CLAY. Thank you very much, Mr. Brachfeld.

We have been joined by two additional Members. I will yield to Mr. McHenry for his opening statement.

Mr. MCHENRY. I thank the chairman.

Ms. Thomas, thank you for agreeing to join us today, this time, for the hearing.

The topic today is, of course, the National Archives and Records Administration organizational issues, but I think that is sort of diminishing the import of this. And organizational issues I think is putting it lightly, the scope or the magnitude of the problem that we are facing.

The National Archives is an agency with an extremely important function. It serves as the keeper of our Nation's valuable records, preserves government and historical records that include copies of acts of Congress, Presidential proclamations and Federal regulations. While the Archives maintains public access to some documents, other records contain highly sensitive data.

Mr. Brachfeld, thank you for touching on the national security component in your testimony.

And these must be secured to ensure our national security and shield personally identifiable information as well. The effectiveness of the Archives as protector of the records under its control is key to preserving our history and maintaining accountability in our government.

The Archives conducts truly invaluable work, very important work, obviously, yet they are an agency that the public doesn't often hear much about. Unfortunately, they have been getting quite a lot of press lately, all of which or most of which seems to be negative. In May, the National Archives Inspector General, Mr. Brachfeld, notified Congress that an external hard drive containing national security information had gone missing from the agency's College Park facility sometime between October 2008 and March 2009, when its absence was first noticed.

That drive contained one terabyte of information, and what we have come to know is that Clinton presidency records, the equivalent of which are millions of books full of information, as Mr. Brachfeld has previously put it. The missing data, including more than 100,000 Social Security numbers, the personal contact information of Presidential administration officials, the entire computer files of 113 former White House employees, Secret Service and White House operating procedures, and other highly sensitive information.

Disturbingly, the missing hard drive was stored in an easily identifiable package, as Ms. Thomas testified to today, in a workspace that the Archives has already admitted was unsecured, unattended, and accessible to personnel without clearance. Even now, it is still not known whether the hard drive was misplaced, lost or stolen, or even when it actually went missing.

It is my hope that the National Archives management would immediately react to what has been called a catastrophic loss by tightening security and accessibility at their College Park facility, particularly in the area which the hard drive was removed.

However, when a bipartisan group of Oversight Committee staff visited the campus on July 17th, they observed many of the same

deficiencies in security measures and left with the impression that a motivated criminal would be able to remove sensitive material with little to no resistance.

Now, this is a bipartisan assessment. There wasn't much of an effort on the part of National Archives staff to even make it appear that substantive changes had been made to secure the location. To be fair, the pattern of material mismanagement of the National Archives precedes Ms. Thomas by quite a few years. We are still remembering Clinton administration official National Security Adviser Sandy Berger caught walking out of the Archives with his pants stuffed, or actually rather socks, stuffed full with classified uninventoried documents.

There are many more alarming cases of negligence at the Archives, yet none as egregious as the disappearance of the hard drive. These include the disappearance of $6 million worth of taxpayer-funded equipment over the periods of 2002 to 2006, the disposal of countless original records from the Bureau of Indian Affairs with the Archives trash, and the disappearance of 55,000 pages of CIA and other Federal agency records right off the shelf in 2006.

There is a prevalent culture of carelessness at the National Archives and it must be replaced with meticulous accounting for all materials, paper and electronic, and stringent security measures that restrict access of unauthorized employees to areas where confidential data is kept.

On Tuesday, President Obama announced he had selected his nominee as Archivist to replace Ms. Thomas, David Ferriero. Quite frankly, I believe this announcement couldn't come soon enough. Mr. Ferriero has certainly had a lot of experience managing mass quantities of paper and electronic documents and other information in his tenure as director of Research Libraries at the New York Public Library, and I look forward to hearing about his qualifications and his plans for the National Archives at his Senate confirmation hearing, whenever the Senate really gets around to doing their job.

And I thank the witnesses for appearing here today, and look forward to the testimony and explanation of how the hard drive full of sensitive information was lost or stolen.

[The prepared statement of Hon. Patrick T. McHenry follows:]

Statement of Congressman Patrick McHenry
Ranking Member
Subcommittee on Information Policy, Census, and National Archives
"National Archives and Records Administration Organizational Issues"
July 30, 2009

Thank you, Mr. Chairman, for holding this very important hearing. And Miss Thomas, I'm glad to see that you were able to make it this time to testify before our Committee.

The topic of today's hearing is "National Archives and Records Administration Organizational Issues" – but I think calling the inherent failures of Archives management to secure and account for stored data "organizational issues" is putting it far too lightly.

The National Archives is an agency with an extremely important function. It serves as keeper of our nation's valuable records, preserving government and historical records that include copies of acts of Congress, presidential proclamations, and federal regulations. While the Archives maintains public access to some documents, other records contain highly-sensitive data, and these must be secured to ensure our national security and shield personally-identifiable information. The effectiveness of the Archives as protector of the records under its control is key to preserving our history and maintaining accountability of our government.

The Archives conducts truly invaluable work, yet they are an agency that the public doesn't often hear much about. Unfortunately, they've been getting quite a lot of press as of late, and none of it good.

In May, National Archives Inspector General Brachfield notified Congress that an external hard drive containing national security information had gone missing from the agency's College Park facility sometime between October 2008 and March 2009, when its absence was first noticed. That drive contained one terabyte of data composed of Clinton presidency records and is the equivalent of "millions of books" full of information, as Mr. Brachfield has previously put it. The missing data includes more than 100,000 social security numbers, the personal contact information of presidential administration officials, entire computer files of 113 former White House employees, Secret Service and White House operating procedures, and other highly-sensitive information.

Disturbingly, the missing hard drive was stored in easily-identifiable packaging in a workspace that the Archives has admitted was unsecure, unattended, and accessible to personnel without clearance. Even now, is still not known whether the hard drive was misplaced, lost, or stolen, or even when it actually went missing.

It was my hope that National Archives management would immediately react to what has been described as a "catastrophic loss" by tightening security and accessibility at their College Park facility, particularly in the area from which the hard drive was removed. However, when Oversight Committee staff visited the campus on July 17, they observed many of the same deficiencies in security measures and left with the impression that a motivated criminal would be able to remove sensitive materials with little to no resistance. There wasn't much of an effort on the part of National Archives staff to even make it *appear* that substantive changes had been made to security.

To be fair, the pattern of material mismanagement at the National Archives precedes Miss Thomas by quite a few years. We all still remember President Clinton's National Security Advisor, Sandy Berger, caught walking out of the Archives with his pants stuffed with classified, uninventoried documents.

There are many more alarming cases of negligence at the Archives, yet none as egregious as the disappearance of the hard drive. These include the disappearance of $6 million dollars of taxpayer-funded equipment over the period of 2002 to 2006; the disposal of countless original records from the Bureau of Indian Affairs with the Archives' trash; and the disappearance of 55,000 pages of CIA and other federal agency records right off the shelf in 2006. There is a prevalent culture of

carelessness at the National Archives, and it must be replaced with meticulous accounting for all materials – paper and electronic – and stringent security measures that restrict access of unauthorized employees to areas where confidential data is kept.

On Tuesday, President Obama announced he had selected his nominee for an Archivist to replace Miss Thomas – David Ferriero. Quite frankly, I believe this announcement could not come soon enough. Mr. Ferriero has certainly had a lot of experience managing mass quantities of paper and electronic documents in his tenure as director of research libraries at the New York Public Library, and I look forward to hearing about his qualifications as well as how he plans to turn around the National Archives at his Senate confirmation hearing.

I thank our witnesses for appearing today and I am very interested to hear an explanation of how the theft of a hard drive full of sensitive information from the National Archives could occur and what sort of measures are being taken to prevent a recurrence.

Mr. CLAY. Thank you, Mr. McHenry.

We will now go into the questioning stage of this hearing, and I will start it off with Ms. Norton for 5 minutes.

Ms. NORTON. Thank you very much, Mr. Chairman.

I see why you called this hearing. It is a virtually mandatory hearing in light of the circumstances and the buildup of the security issues.

Let me make sure what we are talking about, because as I looked at the testimony, I think it is Mr. Brachfeld's testimony, I tore it out, which says the hard drive contained examples of personally identifiable information.

You know, the word secure information has been thrown around in the last several years so loosely. I am trying to understand what was on the hard drive. What does it mean by personally identifiable information?

Mr. BRACHFELD. Is that question directed at me, ma'am?

Ms. NORTON. Yes, Mr. Brachfeld, that is fine.

Mr. BRACHFELD. There is a technical definition for PII. For purposes of this hearing, what I will define is that OMB defines PII material to include Social Security numbers and like material that could be used to damage a person's security, banking, for identity theft, along those lines. It could be names, addresses, associates, that kind of information.

As this information was a compilation from the Clinton administration, it was a compilation, it has information that was resided on individual computers, and thus there is information that meets that definition that resided on the hard drive that is missing.

So again, it was a compilation of material.

Ms. NORTON. Have all of the parties whose information was compromised been so informed?

Mr. BRACHFELD. I will yield to the Acting Archivist.

Ms. THOMAS. We are in the process of identifying the individuals that need to be notified of the breach.

Ms. NORTON. When did the breach occur?

Ms. THOMAS. I am sorry?

Ms. NORTON. When did the breach occur? When was it noted?

Ms. THOMAS. At the end of March, actually on April 2nd it was reported to me, to Mr. Brachfeld, and to Mr. Stern that the hard drive had been lost.

Ms. NORTON. Considering the nature of information and that this is the month of almost August, are you saying that most of these parties have not been so notified?

Ms. THOMAS. We don't at this point know how many people's names and Social Security numbers are on the hard drive.

Ms. NORTON. Why do you not know that information?

Ms. THOMAS. There are 8.7 million individual files on this hard drive, and we have a contractor at this time trying to extract all of the data that they can to come up with the lists to go through——

Ms. NORTON. Is that contractor, like this one, off the premises? This is another contracting out matter where people who apparently should not have been handling secure information were doing so. Now, where is this contractor located and why couldn't this be done on the premises so the hard drive would not have had, why

did the hard drive have to leave the premises, I suppose is my question.

Mr. Brachfeld.

Mr. BRACHFELD. Let me answer your last question. The process of copying the information from White House tapes or what were White House EOP employees' tapes to the hard drive was done offsite and that is what I testified regarding. That was done offsite up in New Jersey, and that is where I have raised significant security issues.

The second part of your interest, which is on now attempting to mine and identify those individuals whose PII may have been compromised, that is under a separate contract which is being administered by the Archives.

The reason it is taking so exceptionally long is this is probably, as far as I know through my 30-year career, this is probably the greatest challenge in trying to identify——

Ms. NORTON. You are having to reconstruct essentially what was on the hard drive with nothing to go on?

Mr. BRACHFELD. What my investigators are trying to do and are now yielding the PII element to the contractor, what we are attempting to do is to use the latest forensic investigative software available. This is not normal data that sits in one standard language or one standard format.

If you think about every record that you have ever captured over your career in different languages and different spread sheets and different formats, all being compressed into one entity. That is what has happened. It is not readily mineable and definable as one would think.

Ms. NORTON. So nobody's been notified as of now?

Mr. BRACHFELD. I yield.

Ms. THOMAS. We have sent I believe it is 15,000, somewhere between 15,000 and 16,000 letters have gone out to notify people of the breach of their information.

Ms. NORTON. Do you have any idea how long it will take before all of the parties have been notified? What kind of harm could be done in the meantime?

Ms. THOMAS. I think it is going to take several months. I think one of the things that this has made perfectly clear to us, it is very difficult to get the information off the hard drive. There are many different——

Ms. NORTON. So you think that in terms of a nefarious act, someone trying to use the data, that would not be very easy to do?

Ms. THOMAS. Given that we have a contractor that was suggested to us by the National Security Agency as somebody that they had worked with, who they thought was the best in the field to try and do this, I do indeed believe that it is going to be difficult for anybody to extract this information from the hard drive.

Ms. NORTON. Well, Mr. Brachfeld, you said a criminal investigation is going on. Is there any possibility other than this being stolen that you would regard as a credible possibility? I mean, could it have been mislaid? If it had been mislaid, where would that have been, since there were only two places it should be, either the Archives or with the contractor?

Mr. BRACHFELD. I cannot dismiss any aspect as to whether or not it is missing, somebody took it for purposes of benign intent, just to use it for their own medium, or the worst case scenario, that it was taken for more nefarious purposes. That is a potential.

I also want to state that people with the correct technologies and tools can mine this data. We have a contractor now that is trying to, my investigation is focusing on how it happened and what the impact of the loss is, and if we can find the subject.

I am also looking at what classified material resided on that hard drive and other sensitive information. I am no longer involved in looking at the PII content. That has now been yielded to the contractor working for the National Archives.

What I can say is, again, people with the capacity to read this data, the tools, can do it. My investigators, my forensic auditor could in fact pull up PII information fairly readily. Now, to find the tremendous quantity to issue PII letters, as the agency is doing, that is another subject. But certainly, somebody with, if they had that intent, and if in fact it really is out there and somebody is using it for that purpose, certainly they could pull P.I. information off of that drive.

Ms. NORTON. Mr. Chairman, could I just ask to the extent that there is a discovery of criminal use of this information that the chairman of this subcommittee be informed immediately? I don't know what people could do to protect themselves, but I think the worse thing to happen in a circumstance like this is not to even know that out there in the stratosphere and perhaps in the hands of thieves is all your personal information.

And if it is discovered, it seems to me at such point it is discovered, if you are at 20,000 of 8 million or whatever, it seems to me that this committee should be informed at that point.

Mr. CLAY. Oh, for certain that will be made part of this official hearing record.

Ms. NORTON. Thank you very much, Mr. Chairman.

Mr. CLAY. Thank you for the question.

Mr. McHenry, are you ready?

Mr. MCHENRY. Yes.

Ms. Thomas, how long have you been Acting Archivist?

Ms. THOMAS. Since mid-December 2008.

Mr. MCHENRY. Since mid-December.

Mr. Chairman, I am not familiar with most administration officials testifying with counsel at the desk. It seems to me a bit telling about the situation we are in, about how sensitive this is. But you know, Ms. Thomas, I know this predates you. I mean, this doesn't necessarily simply fall at your feet. So I mean, how long have you been with the Archives?

Ms. THOMAS. Thirty-nine years.

Mr. MCHENRY. Thirty-nine years, full career. So you know, there have been studies on job satisfaction within the Federal Government. And I think it was American University's Best Places to Work in the Federal Government 2009, American University's Institute for the Study of Public Policy. Are you familiar with the study?

Ms. THOMAS. Yes.

Mr. MCHENRY. Yes. It was telling to me, based on our Oversight Committee, to see where National Archives and Records Administration ranks. It is extraordinarily low in terms of job satisfaction within the Federal Government. It is actually, I think the second to last of all the institutions they studied.

Do you think there is a linkage between job satisfaction—well actually, let's start here. What do you attribute the low job satisfaction assessment to?

Ms. THOMAS. Well, we did some further analysis of what the different rankings were in the different parts of the National Archives. And the truth of the matter is that most of the very low rankings came from our regional facilities. And we have, for example, in our Federal Records Centers, which are fairly low paid occupations, they are not exactly intellectually stimulating.

It is people moving boxes in and out and so forth. There is not a whole lot of promotion potential within the Records Center system, and a great deal of the very low scores in terms of job satisfaction came from those regional activities.

If you look at the National Archives in the Washington area, we rank at at least the same average as most other agencies or a little higher. So the regional scores basically bring the agency score down to the level that is reported in that study.

Mr. MCHENRY. OK. OK. Do you think that there is any linkages between dissatisfaction and disappearance of records or theft of records?

Ms. THOMAS. I think there could be, but the averages for the people who are working with archival records are much higher and they are not low. The Records Center records, of course, are agency records, temporary records, not archival records. So the incidents that have occurred over the past several decades have occurred in archival records.

Mr. MCHENRY. OK.

Ms. THOMAS. So I am not sure that the linkage is there.

Mr. MCHENRY. In terms of your testimony, you said that this drive with one terabyte of information was kept in its original package. Is that true?

Ms. THOMAS. Yes, that is correct.

Mr. MCHENRY. OK. Is that standard procedure within your division of government to put these objects back in their original box?

Ms. THOMAS. In most cases, information——

Mr. MCHENRY. If you don't have a policy, then that is fine, then if you will just state that.

Ms. THOMAS. I don't know. I can provide that for the record. I don't know the answer.

Mr. MCHENRY. Yes, if you could, that would be good.

Ms. THOMAS. Sure.

Mr. MCHENRY. It seems somewhat bizarre to me to have such important information, and this is not really judging the information. You know, but having it lost to history is a major concern and being able to piece this back together on what the——

Ms. THOMAS. Well, the information is not lost because this was a backup tape. It is a copy.

Mr. MCHENRY. OK. Where was the original kept? Wasn't it all in the same desk?

Ms. THOMAS. The originals are the tapes that were delivered from the EOP at the end of the Clinton administration. Those tapes were backed up onto these hard drives, one of which was a master hard drive and one which is a copy hard drive.

Mr. MCHENRY. And they were next to each other?

Ms. THOMAS. Yes, but the tapes were stored in the locked staff area, the original records.

Mr. MCHENRY. OK. Is there a procedure for having a master, the original and the backup, the two drives, is there a process to keep them separate? If you have the backup and the main drive, right? Same information, is there any policy you have within the Archives to keep them in separate locations?

Ms. THOMAS. Not while they are being processed, and that is what was happening at the time that the hard drives were there.

Mr. MCHENRY. Is it not true that the reason why we don't know if it is October or March is because they have been sitting on someone's desk the whole time and they were not being processed? They were left out untouched.

Ms. THOMAS. I think it is unclear how long they were left untouched.

Mr. MCHENRY. OK, which tells me you don't have any policies or procedures on how this works.

Mr. Brachfeld, are there policies and procedures on paper within the Archives about how to handle two copies of the same data?

Mr. BRACHFELD. I will answer your question by getting specific in this matter. In this case, I should note that drives that were not used new were maintained in a locked area. Whereas the drives that were in process and therefore holding the kind of data and quality of data we talked about today were left in an unlocked, exposed area, put back in the original box.

So to me, it seemed curious and bothersome, troublesome that clean tapes are locked up for security, but tapes that have documentation were left in an open area.

As far as policy and procedures, I guess more specifically, that is what we are investigating. Right now, my focus is investigating a potentially criminal act. We have time and we will look at audit issues. We will look at new internal controls. I can simply say, as I said in my testimony, it would seem that internal controls were not the focus in this area.

Mr. MCHENRY. Well, thank you for your testimony. My time is up, but it seems to me that the basic Archives procedure was the equivalent of putting your car keys and your backup car key on the same key chain. It seemed that it was very basic procedure that was not instituted, nor was there a culture of following those procedures to ensure that you have two pieces of data—right?—kept separately, both secure so that therefore you have in this new technology age that we have, with diminishing documents from the early 1990's as that technology is getting older, that you would actually have those policies and procedures.

So, you know, to the larger issue here is making sure this doesn't happen again for any administration or any document.

And with that, I yield back.

Mr. CLAY. Thank you, Mr. McHenry.

It begs the question of the backup system, that there be a foolproof backup system. Let me ask both witnesses, do you know anything about hundreds of thousands of veterans' PII that has been compromised when the National Archives sent unencrypted hard drives to a vendor in return for replacement of hard drives? And if you do, what has been done to inform veterans that their information has been compromised? Either one.

Mr. BRACHFELD. I will answer that by saying we are in the process, as I stated in my last semiannual report, of conducting an investigation specific to that matter. At this time, I do not have information to the extent that I could respond fully to that question.

We do believe an event occurred. The question is, what is the nature of the event and what are the implications? We are currently investigating that matter.

There have also been other issues related to and have been reported in a management letter, related to St. Louis and the military veterans records in terms of other PII policy and procedures that have been violated that also potentially compromises veterans' information. And again, that is an issue which I cannot discuss in a public forum because should that information be made available publicly, it could be damaging.

So I respectfully cannot—I don't think you would want me to discuss this in this public forum.

Mr. CLAY. OK. Well, I will go to my next witness, and ask Ms. Thomas, can you shed any light on it? Are you aware of it?

Ms. THOMAS. I am unfamiliar with an incident relating to veterans' records and a hard drive and missing records. I just don't have any information on that.

Mr. CLAY. OK. All right. Ms. Thomas, in June 2006, the Information Security Oversight Office inspected the information security controls of NARA's Washington National Records Center. ISOO found that due to inadequate records management, hundreds of boxes of classified materials could not be readily located.

It is my understanding that since the ISOO inspection, NARA has taken steps to improve security at the Washington National Records Center. What is the status of those missing boxes and what has NARA done to improve the management of classified and other materials at the Washington National Records Center?

Ms. THOMAS. There are two vaults at the Washington National Records Center. One contains top secret SCI and R.D. material, and the second vault contains secret and confidential information.

The Washington National Records Center has almost four million cubic feet of records. Of those, 333,000 are classified, either at the top secret SCI or secret or confidential.

The controls, the ISOO made recommendations, 22 different recommendations for how to improve security at the Washington National Records Center. At this stage, I believe all of them have been implemented. An Information Security Program Manager has been hired. A Vault Manager has been hired. Resources have been thrown into the Records Center to do a complete inventory of both vaults.

They started on the top secret and the SCI one. And they completed that inventory. Initially, they found 1,400 boxes that were not where they were supposed to be. They then did a complete

check and got that number down to, I believe, 125 boxes of material that is not apparently on the shelves at the Washington National Records Center.

These records are owned by the agencies. They are not NARA records. They are not archival records. They are often called back by the agencies. And often what has happened in the past is that an agency calls back records and they either keep them, because they are their records and they have that right, and/or they will send them back some months or years later in another accession so that the number changes in terms of how you identify the records, and they get shelved as a new accession, and they contain boxes from the old accession.

So there certainly was a record keeping issue that needed to be straightened out so we could keep better control over what went back to the agency, whether they were permanently withdrawn and kept in the agency, or whether or not they were returned to the Washington National Records Center.

We are now, for the 125 boxes that are still not accounted for, we have contacted six different agencies whose records these are and asked them if they could check and find out if perhaps they have a record of whether or not they borrowed back these records. I believe there was something from the Energy Department just in the past few weeks that said, oh yes, they have 15 of the boxes that they have been able to account for.

So we are still working the process to find out where the records are, and a similar inventory of the secret and confidential vault is underway. And we will go through the same process of completing the inventory, determining to the best we can where the records are, and whether or not they have been loaned back to the agencies or permanently withdrawn by the agencies.

Mr. CLAY. OK. And thank you for your response.

Mr. McHenry's second round of questioning.

Mr. MCHENRY. Certainly. Thank you, Mr. Chairman.

Now, you found out about this security breach, or the disappearance of the drive April 2nd, you said. Is that correct?

Ms. THOMAS. Yes. That is when I was informed.

Mr. MCHENRY. OK.

Ms. THOMAS. All three of us were informed. Gary is here because he is the Privacy Officer for the agency and has responsibility for PII.

Mr. MCHENRY. So what have you done to address this so it doesn't happen again?

Ms. THOMAS. The Office of Record Services for Washington did a complete review of procedures, and has implemented much more stringent procedures to make sure that it doesn't happen again. Some of them I went through in my testimony, and they are in more detail in my longer testimony that is submitted for the record.

Mr. MCHENRY. Yes.

Ms. THOMAS. They have put card readers on doors where before you could go into the office area and then go into the processing area. The card reader on the office door would, in essence, get you into the office area and into the processing office. Now, the process-

ing space has another layer of security, and so you have different card reader access for those doors.

They are doing spot inspections. The supervisors and managers are going through the space to make sure that the procedures that we put in place are being adhered to.

We intend to do more training for people so that they truly get the message that this is a basic part of their job is protecting the records that they are working with. And that is a balancing act between providing access for research purposes and securing the items, but securing the items is a critical, critical part of their job.

Mr. MCHENRY. Certainly. Now, are you familiar with the Inspector General's audits from between October 2007 and March 2008? Are you familiar with the audits that the Inspector General's office issued?

Ms. THOMAS. Well, I see the audits, yes.

Mr. MCHENRY. OK. Because at that point, it was pointed out in that audit that the Archives was, "not accounting for artifacts in a timely manner." That was one. And two, among other things, artifacts were "not maintained in appropriate space."

So the audit there expressed some of the same failings that resulted in the disappearance of this data. Did you have any actions you took off that audit from——

Ms. THOMAS. Well, I think that audit referred to the museum items, the artifacts in Presidential libraries.

Mr. MCHENRY. Yes.

Ms. THOMAS. And Presidential libraries had started an inventory process. It was at various stages in the different libraries. We indeed poured more resources into completing the inventories, and they are underway. Some of them have been completed. Some of the problems that existed in the older libraries will not exist for the Bush Library or any library going forward because there will be a computer system that tracks every artifact as it arrives in the White House, and then that system is provided to us so that we will have a complete list to start out with.

The record keeping in the White House Gift Office wasn't as complete in the past, and it was not consistent, if I can give you an example. A tea set, is that one item or is that a teapot and four cups? And is there a tray? Is that seven items? You know, there was no consistency in how they dealt with it.

Mr. MCHENRY. But within one division of the Archives, when you have issues like, you know, not having information secured in appropriate space, does that raise questions for the overall system? Do you look at overall systems within the Archives? Or is that just one division and therefore isn't applicable to anywhere else?

Ms. THOMAS. For the issue with the hard drive, we are going to undertake a complete review. The Office of Records Services in Washington has already started.

Mr. MCHENRY. I thought you said they have already done that.

Ms. THOMAS. I am sorry?

Mr. MCHENRY. I thought you said, in my last question, that they had already done a complete review.

Ms. THOMAS. They did it for the Electronic Records Division. They are branching out to all of their records holding units and, as you said, looking at it more holistically across the agency, as op-

posed to just in one division. So we are looking at all security procedures and whether or not they are sufficient, whether they need to be improved.

We certainly have decided that we need to improve our training and that we need training at a lot of different levels. For example, I am proposing that we will train every employee that comes to the National Archives as part of their orientation, whether they are a budget analyst or whatever, to make them understand what the mission of the agency is and that everybody has a responsibility to make sure that records are protected.

Mr. MCHENRY. Thank you. Thank you. Very good answer. Thank you.

Mr. CLAY. Ms. Thomas, regarding the notices that were sent out to the 16,000, roughly, people, were there any problems with the notices? I have received reports that recipients of those notices thought that they were scams.

Ms. THOMAS. We did have some questions come in. We had a hotline set up for any questions that anybody did have. And we also had an email box where they could contact us. And yes, the most frequently asked question that came to us was: Is this a scam? Is this somebody who is, you know, Prince so and so from somewhere who is, you know, trying to get hold of my personal information and drain my bank account or something?

So we have answered those questions.

Gary, if you have anything to add to that?

Mr. CLAY. Mr. Stern.

Mr. STERN. I can try. Yes.

The letters were sent out by our contractor providing the credit monitoring services as well. And so while it is on NARA letterhead, it was put in an envelop that looks more like the kind of envelope you get from, you know, a bank or something else.

Mr. CLAY. A solicitation?

Mr. STERN. Exactly. So I think some people thought, weren't sure, is this really from the National Archives or is this just some company just trying to, you know, solicit my business. And so we assured those people that it really was from us. We referred them to our Web site and we put up an updated notice to say we have sent these letters out and they are legitimate, and we are informing you of this potential breach and offering this service.

So there was some confusion that we just hadn't occurred to us that would result by sending out the letters in that format.

Mr. CLAY. I see.

Any recommendations, Mr. Brachfeld?

Mr. BRACHFELD. Specific to that question?

Mr. CLAY. Yes.

Mr. BRACHFELD. I am pretty much apart from that process. Again, my duty is to do the investigations. We reviewed the language in the breach notification letter just as a courtesy and the language in the breach notification seemed to be appropriate.

As far as the contractor, the mailing, that is completely outside of my domain.

Mr. CLAY. So there was really two mailings. Did you re-mail the notices or no?

Ms. THOMAS. No, no, no. But there was an email box set up and in the letter that notified people of the breach, they were provided with the email address. They were provided with a hotline number that they could call. And they were notified that they could look at our Web site for further information, so that if they had any questions about the breach notification, they could contact us in several different ways.

Mr. CLAY. Ms. Thomas, regarding the copying of Executive Office computer tapes onto this hard drive, why were security requirements not built into the contract documents with your vendor?

Ms. THOMAS. Well, the contractor that did the work on the latest batch of copying, because there were five different contracts, I believe, for various stages of copying of this material, was a GSA schedule contract with the routine, I will say routine, because they were, clauses about protection of government information, government products that were provided to the contractor.

In hindsight, our people should have included some additional security requirement clauses in the contract and that will certainly be a part of any contract going forward.

Mr. CLAY. OK.

Mr. Brachfeld, any comment on that?

Mr. BRACHFELD. I have pretty much all the documentation related to this contract and what is clearly missing is any, any mention of security as even a consideration within the body of any of the solicitation.

The company that received the tapes did not even respond in terms of their having any security arrangements in place. Again, there was no clause for nondisclosure of information, as should be customary in such a contractual relationship, contractual document.

Basically, it just shouldn't have happened, and I think the Archives will learn from that.

Mr. CLAY. This sounds pretty sloppy as far as how we handle sensitive information.

Mr. BRACHFELD. We visited the site and it is not the contractor's fault, per se, because the contractor was doing a duplication service. They were honoring the terms of the contract. But if you went to the contractor site, as my agents did, along with other law enforcement you would have seen a basic storefront operation with security clearly not the focus. You would see that the tapes were kept in a room where doors were propped open also.

I have actually images of this and it will be in my investigative report when it is finalized, or I could present them to you subsequent to this hearing. It was not the environment that one would expect you would keep something of even minimal importance, much less the quality and quantity of data that we have discussed today.

Mr. CLAY. You can certainly share whatever information you can with this subcommittee, so that we can get a clear picture of it.

Mr. BRACHFELD. I will do that.

Mr. CLAY. I will stop there and let Mr. McHenry have the last question.

Mr. MCHENRY. Mr. Chairman, I thank you for having this hearing. I think it is important that we get the right policies and proce-

dures in place. And this is not necessarily an adversarial thing, I am just perplexed at how something so basic could disappear. You know, these hard drives in my experience aren't cheap to get anyway. They are not cheap objects to have lying around, much less with no information, much less with sensitive information on it.

And so it seems to me that even so much as actually taking that hard drive, instead of leaving it out, putting it in a locked desk drawer would have been a world apart from what happened, or as near as we can tell, happened with the minimal amount of information that is actually known right now.

And as the IG still has the investigation going on, and I would love to have any information as you produce it that you are able to share with us, we would certainly appreciate it.

Mr. Chairman, thank you for having this hearing and thank you for your leadership.

Mr. CLAY. Thank you, too, Mr. McHenry.

Since there are no further questions, that concludes this hearing.

The committee is adjourned.

[Whereupon, at 3:44 p.m., the subcommittee was adjourned.]